

09744781.41500

1 ABSTRACT

2 A system collects entropy data and stores the entropy data in a nonvolatile
3 memory. The entropy data stored in the nonvolatile memory is updated with
4 newly collected entropy data. The entropy data stored in the nonvolatile memory
5 is used to generate a string of random bits. The entropy data is collected from
6 multiple sources within a computer system and may include data related to a
7 processor in the computer system and an operating system executing on the
8 computer system. The entropy data is maintained in a protected portion of an
9 operating system kernel. A hashing algorithm is applied to the entropy data to
10 generate random seed data.
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25